(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특2001-0027902
H04L 9/32		(43) 공개일자	2001년04월06일
(21) 출원번호	10-1999-0039881		
(22) 출원일자	1999년09월16일		
(71) 출원인	주식회사 데이타웨이브 시스템, 박진우		
	대한민국		
	135-877		
	서울 강남구 삼성2동 143-20 경원빌딩 6층		
(72) 발명자	권태경		
	대한민국		
	140-202		
	서울특별시용산구이태원2동남산대림아파트110동104호		
(77) 심사청구	없음		
(54) 출원명	사용자가 기억할 수 있는 패스워드를 이용한 안전한 사용자 인증과 키 일치 방법		

요약

본 발명은 인터넷과 같이 다수의 사용자가 다양한 서비스를 이용하게 되는 공중망 환경에서도 일반사용자가 기억할 수 있는 패스워드(password)만을 통해서, 안전하게 사용자 인증(user authentication) 및 Diffie-Hellman 키 일치(key agreement)를 이룰 수 있도록 하는 방법을 대상으로 한다. 본 발명은 네 단계의 절차를 갖는 인증 프로토콜과 이를 이용한 온라인 등록 절차를 함께 포함한다. 본 발명의 인증 프로토콜을 통해서는 패스워드에 의한 사용자 인증과 함께 Diffie-Hellman 지수(g^(xy)(mod p))를 키로서 안전하게 일치할 수 있다. 또한, 서버는 사용자 아이디와 솔트처리된 패스워드(salted password)만을 저장하여 패스워드 파일의 안전성을 도모하고, 사용자는 아이디와 함께 기억가능한 패스워드만을 입력하여 간편하게 인증을 받도록 한다. 특히 인증에 실패할 경우 뿐만 아니라 성공할 경우에도 실제 패스워드에 대한 정보가 유출되지 않도록 한다. 인증 프로토콜을 활용하여 사용자는 자신의 아이디와 패스워드를 온라인으로 서버에 등록할 수 있도록 한다.

대표도

도3

색인어

암호, 보안, 사용자 인증, 인증 프로토콜, 키 일치, 공개키, 패스워드, 솔트, Diffie-Hellman

명세서

도면의 간단한 설명

도 1 - 인증구조 초기화 방법

도 2 - 패스워드 온라인 등록 방법

도 3 - 사용자 인증 방법

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명이 속하는 기술분야는 컴퓨터 통신망 보안기술, 그 중에서도 패스워드 기반 사용자 인증 기술분야다.

이 분야의 종래기술로서 사용자 인증 방법은 사용자가 기억할 수 있는 패스워드나 개인식별번호를 이용하는 지식기반인증, 사용자가 소지하는 자기카드(magnetic card)나 스마트카드(smart card)를 이용하는 토큰기반인증, 그리고 사용자의 생체학적 특징, 즉 지문이나 망막구조 등을 이용하는 생체기반인증으로 분류된다. 또한 지식기반인증과 토큰기반인증의 특성을 결합한 패스코드카드 인증기법 등이 있다. 그 중에서도, 인터넷과 같은 공중망에서는 구현의 경제성과 용이성으로 인하여 사용자가 기억할 수 있는 패스워드를 통한 사용자지식기반인증이 주로 사용되어왔다. 그러나 이와 같은 방법은 통신망상에서 패스워드를 안전하게 전송하고 관리하기 어렵다는 문제점을 갖는다.

이와 같은 패스워드의 안전성 개선을 위해서 패스구문(passphrase)[1], 일시패스워드(one-time password)[2], 공개패스워드(public password)[3], 패스코드카드[4] 그리고 패스워드 인증 프로토콜[5] 등의 종래 기술들이 개발되었으나, 패스구문은 사용자가 기억해야 하는 단어의 수가 크게 많아지는 단점을, 그리고 일시패스워드나 공개패스워드, 패스코드카드는 사용자가 패스워드를 기억할 뿐만 아니라 패스워드리스트나 패스코드카드를 별도로 소지해야 하는 단점을 갖는다. 한편 패스워드 인증 프로토콜은 인증된 공개키 요구, 많은 난수의 생성, 그리고 많은 암호학적 연산이나 프로토콜 단계로 인하여 많은 비용을 요구한다. 또한 커베로스(Kerberos)와 같은 인증시스템은 결정적으로 패스워드의 안전성을 제공하지 못한다[6].

특히 패스워드 프로토콜의 가장 큰 문제점은 솔트처리된 패스워드(salted password)[1]를 사용할 수 없다는 점이다. 하지만 EKE(Encrypted Key Exchange) 프로토콜[7]을 개선한 A-EKE(Augmented-EKE) 프로토콜[8]은 솔트처리된 패스워드를 사용할 수 있도록 하여 패스워드 파일에 대한 안전성을 더욱 강화하였다. 또한 Diffie-Hellman 문제의 안전성[9]에 근거해서 키 일치를 이루도록 한다. 하지만 A-EKE는 전자서명을 포함한 일곱 단계로 이루어진 높은 비용의 프로토콜이다. 따라서 A-EKE의 성능을 개선한 B-SPEKE 프로토콜[10]과 SRP[11] 프로토콜이 가장 중요한 종래 기술로 언급될 수 있다. 하지만, B-SPEKE는 다섯 단계로 이루어졌으며, 소수 p의 선택을 위한 제한(p=2q+1 for $'q$)이 따른다. 또한 SRP는 네 단계로 이루어진 반면, 정확한 Diffie-Hellman 키 일치를 제공하지 않는다.

본 발명에서는 네 단계로 이루어진 프로토콜을 통해서 사용자 인증과 정확한 Diffie-Hellman 키 일치를 이루는 방법을 대상으로 한다.

[1] D.Feldmeier and P.Karn, ``UNIX password security - ten years later,'' in Proc. Crypto 89, Springer LNCS 435, 1990, pp. 44-63.

[2] Haller, ``The S/Key one-time password system,'' in Proc. Symp. Network and Distributed System Security, San Diego, California, 1994.

[3] S.Halevi and H.Krawczyk, ``Public-key cryptography and password protocols,'' in Proc. ACM Conf. Comp. and Commun. Security}, Nov. 1998, pp. 122-131.

[4] http://www.activcard.com/products/BMAS-ActivCard/index.html

[5] L.Gong, M.Lomas, R.Needham, and J.Saltzer, ``Protecting poorly chosen secrets from guessing attacks,'' IEEE J. Select. Area Commun., vol. 11, no. 5, pp. 648-656, June 1993.

[6] T.Wu, ``A real world analysis of Kerberos password security,'' Internet Society Symp. on Network and Distributed Sys. Security, 1999.

[7] US5241599: Cryptographic protocol for secure communications (invented by S.Bellovin and M.Merritt, AT&T)

[8] US5440635: Cryptographic protocol for remote authentication (invented by S.Bellovin and M.Merritt, AT&T)

[9] W.Diffie and M.Hellman, ``New Directions in Cryptography,'' IEEE Transactions on Information Theory, Vol.22, No.6, pp.644-654, Nov. 1976.

[10] D.Jablon, ``Extended password key exchange protocols,'' WETICE Workshop on Enterprise Security, 1997.

[11] T.Wu, ``Secure remote password protocol,'' Internet Society Symp. on Network and Distributed Sys. Security, 1998.

발명이 이루고자 하는 기술적 과제

본 발명은 사용자가 기억할 수 있는 짧은 문자열, 즉 패스워드만을 통해서 안전한 사용자 인증과 암호키 일치를 이루도록 한다. 따라서 다음과 같은 기술적 과제를 해결하도록 한다.

1. 네 단계의 패스워드 인증 프로토콜을 통해서 Diffie-Hellman 지수 $g^{xy}(\mathrm{mod}p)$를 키로서 안전하게 일치할 수 있도록 한다.

2. 소수 p를 선택할 때 안전한 소수 p=2q+1 for $'q$ 조건을 완화하여, non-smooth 소수로도 만족하도록 한다.

3. 서버는 사용자 아이디와 솔트처리된 패스워드만을 저장하고, 사용자는 아이디와 함께 기억가능한 패스워드만을 입력하여 인증을 받도록 하지만, 인증에 실패할 경우 뿐만 아니라 성공할 경우에도 실제 패스워드에 대한 정보가 유출되지 않도록 한다.

4. 인증 프로토콜을 활용하여 사용자가 자신의 아이디와 패스워드를 온라인으로 서버에 등록할 수 있도록 한다.

발명의 구성 및 작용

본 발명의 대상은 인증구조 초기화, 사용자 패스워드 온라인 등록, 그리고 사용자 인증의 세 단계의 방법으로 이루어진다. 인증구조는 사용자가 직접 사용하게 되는 클라이언트 응용부와 사용자를 인증하는 서버 응용부로 구성되며, 사용자 패스워드 온라인 등록과 사용자 인증을 위해서는 두 응용부가 서로 정해진 연산을 통해서 정해진 메시지를 네 단계로 주고 받게 된다.

1. 인증구조 초기화 방법

도 1

본 발명의 인증구조 초기화는 [도해 1]과 같이 이루어지며, 클라이언트 응용부와 서버 응용부가 해당 모듈을 포함하게 된다. 본 발명의 인증 방법을 사용하기 위해서는 이와 같이 초기화된 클라이언트 응용부와 서버 응용부를 설치한다.

① 클라이언트 응용부와 서버 응용부는 각각 모듈러 멱승 모듈을 포함한다.

② 클라이언트 응용부와 서버 응용부는 큰 정수 연산(가,감,승) 모듈을 포함한다.

③ 클라이언트 응용부와 서버 응용부는 강한 성질의 일방향 해쉬함수와 이를 이용하는 간단한 함수로 구성된 함수 모듈을 포함한다.

④ 클라이언트 응용부와 서버 응용부는 기본 연산(XOR) 모듈을 포함한다.

⑤ 클라이언트 응용부와 서버 응용부는 암호학적으로 안전한 의사난수발생기(pseudo-random number generator) 모듈을 포함한다. 이 모듈은 패스워드(s)와 같은 크기의 난수(t)와 작은 난수(a)를 생성하며, $1<r,x,y<p-1$ 범위에서 큰 난수(r,x,y)를 생성한다.

⑥ 클라이언트 응용부와 서버 응용부는 블록 암호화 모듈을 포함한다.

⑦ 클라이언트 응용부와 서버 응용부는 송수신 모듈을 포함한다.

⑧ 클라이언트 응용부와 서버 응용부는 암호학적으로 안전한 소수 p를 포함한다.

⑨ 클라이언트 응용부와 서버 응용부는 유한체(finite field) GF(p)의 원시근(primitive root) g를 포함한다.

⑩ 클라이언트 응용부는 1<z<p-1의 범위에서 선택된 큰 난수 z를 유한체안에서 원시근 g에 멱승한 값, $g^z(\mathrm{mod}p)$를 포함한다.

⑪ 서버 응용부는 1<z<p-1의 범위에서 선택된 큰 난수 z를 포함한다.

⑫ 클라이언트 응용부는 사용자 아이디와 패스워드를 입력할 수 있는 사용자 인터페이스를 포함한다.

⑬ 서버 응용부는 패스워드자료를 저장할 수 있는 저장공간을 포함한다.

2. 패스워드 온라인 등록 방법

도 2

본 발명의 패스워드 온라인 등록 방법은 [도해 2]와 같이 이루어지며, 사용자는 클라이언트 응용부를 통해서 서버 응용부에 자신의 아이디와 패스워드를 온라인으로 등록하게 된다. 온라인 등록은 방법은 다량의 연산과 함께 사용자 인증 방법을 포함하며 따라서 보다 많은 시간을 요구하지만, 안전하게 온라인 등록을 할 수 있다.

① 사용자는 자신의 아이디(id)와 패스워드(s)를 선택한 후 클라이언트 응용부의 사용자인터페이스를 통해서 입력한다.

② (i)클라이언트 응용부는 1<r<p-1의 범위에서 임의의 큰 난수 r을 선택한 후 유한체안에서 원시근 g에 멱승($g^r(\mathrm{mod}p)$)하고 또한 저장된 값 $g^z(\mathrm{mod}p)$에 멱승($(g^z)^r(\mathrm{mod}p)$)한다. (ii)클라이언트 응용부는 함수 k1()을 값($g^{zr}(\mathrm{mod}p)$)에 적용한 후 패스워드(s)와 XOR 연산하고, 이렇게 연산한 값(s XOR $g^{zr}(\mathrm{mod}p)$)을 함수 k2()를 값($g^{zr}(\mathrm{mod}p)$)에 적용한 값을 키로 사용하여 블록암호화한다. 함수 k1()과 k2()는 간단한 함수로서, 같은 입력 값에 대해서 서로 다른 값을 생성한다. (iii)클라이언트 응용부는 암호화한 값을 아이디 및 값($g^r(\mathrm{mod}p)$)와 함께 서버 응용부에게 전달한다. (iv)서버 응용부는 저장된 값(z)를 수신한 값($g^r(\mathrm{mod}p)$)에 멱승한 후 값($(g^r)^z(\mathrm{mod}p)$)에 함수 k1()과 k2()를 적용해서 수신한 암호문을 복호화하여 패스워드(s)를 얻는다.

③, ④, ⑤ 서버 응용부는 난수(t)를 생성해서 솔트값으로 사용하기 위해 패스워드(s)와 XOR한 후(s XOR t), 단계 ②-(iv)에서 복호화된 패스워드(s)의 확인을 위해서 사용자 인증 방법의 세단계를 수행한다. 단지 여기서 프로토콜의 난수(a)를 1로 고정(a=1)한다. 프로토콜에 대한 자세한 설명은 발명의 구성 3항의 사용자 인증 방법에서 다루도록 한다.

⑥ 인증 프로토콜이 성공적으로 종료하는 경우 솔트처리된 패스워드로서 값(s XOR t) 및 값($g^v(\mathrm{mod}p)$)를 사용자 아이디(id)와 함께 저장한다. 값(v)는 패스워드(s)와 솔트(t)를 정해진 함수 f()에 입력한 값이며, 함수 f()는 일방향 해쉬함수를 이용하여 설계되는 간단한 함수로서 지수의 비트길이를 Pohlig-Hellman 이산대수분해에 대해서 안전하도록 만드는 역할을 한다. 함수의 자세한 설계는 발명의 구성 3항의 사용자 인증 방법에서 다루도록 한다.

3. 사용자 인증 방법

도 3

본 발명의 사용자 인증 방법은 [도해 3]과 같이 이루어지며, 사용자는 클라이언트 응용부에 아이디(id)와 패스워드(s)만을 입력해서 인증받게 된다.

① 사용자는 기억하고 있는 패스워드(s)를 자신의 아이디(id)와 함께 클라이언트 응용부의 사용자인터페이스를 통해서 입력한다.

② (i)클라이언트 응용부는 난수(a)를 선택하고 아이디(id)와 함께 서버에게 전송한다. (ii)클라이언트 응용부는 1<x<p-1 범위에서 난수(x)를 선택한 후 원시근(g)에 멱승($g^x(\mathrm{mod}p)$)한다.

③ (i)서버 응용부는 아이디(id)를 색인키로 사용해서 저장된 값(s XOR t)와 값($g^v(\mathrm{mod}p)$)를 읽어들인다. (ii)서버 응용부는 1<y<p-1 범위에서 난수(y)를 선택한 후 원시근(g)에 멱승($g^y(\mathrm{mod}p)$)하고, 수신한 값(a)와 값($g^v(\mathrm{mod}p)$)를 곱한 후, 두 결과값을 더한 값($g^y+a*g^v(\mathrm{mod}p)$)을 값(s XOR t)와 함께 클라이언트 응용부에게 전송한다. (iii)서버 응용부는 값(y)를 값($g^v(\mathrm{mod}p)$)에 멱승($(g^v)^y(\mathrm{mod}p)$)한다.

④ (i)클라이언트 응용부는 값(s XOR t)로부터 솔트값(t)를 구한 후((s XOR t) XOR s = t) 사용자 패스워드(s)와 솔트값(t)를 함수f()에 적용하여 값(v)를 생성한다. 함수 f()는 강한 성질의 일방향 해쉬함수 h()를 이용하는 간단한 함수로서 f(s,t)=h(t,h(s,t)),h(s,t)와 같이 구성되어 값(s)와 값(t)로부터 값(h(t,h(s,t)),h(s,t))를 생성한다. (ii)클라이언트 응용부는 값(v)를 원시근(g)에 멱승하여($g^v(\mathrm{mod}p)$) 값(a)와 곱한 값($a*g^v(\mathrm{mod}p)$)을 수신된 값($g^y+a*g^v(\mathrm{mod}p)$)에서 감산($g^y+a*g^v-a*g^v(\mathrm{mod}p)=g^v(\mathrm{mod}p)$)해서 값($g^y$

)를 구한다. (iii)클라

이언트 응용부는 값($g^y(\mathrm{mod}p)$)에 값(v)를 멱승($(g^y)^v(\mathrm{mod}p)$)하여 값($g^x(\mathrm{mod}p)$)와 더하고($g^x+(g^y)^v(\mathrm{mod}p)$), 값($g^y(\mathrm{mod}p)$)에 값(x)를 멱승($(g^y)^x(\mathrm{mod}p)$)하여 값($g^y+a*g^v(\mathrm{mod}p)$)와 값($(g^y)^x(\mathrm{mod}p)$)의 해쉬값(hash1)을 구한다. (iv) 클라이언트 응용부는 값($g^x+(g^y)^v(\mathrm{mod}p)$)와 해쉬값(hash1)을 서버 응용부에게 전송한다.

⑤ (i)서버 응용부는 수신된 값($g^x+(g^y)^v(\mathrm{mod}p)$)으로부터 값($(g^v)^y(\mathrm{mod}p)$)를 감산하여 값($g^x(\mathrm{mod}p)$)를 구한다. (ii)서버 응용부는 값(y)를 값($g^x(\mathrm{mod}p)$)에 멱승하여($(g^x)^y(\mathrm{mod}p)$) 해쉬값(hash1)을 구해서 수신된 해쉬값과 비교한다. (iii)서버 응용부는 값이 일치할 경우 사용자를 인증하고 키($g^{(xy)}(\mathrm{mod}p)$) 일치 사실을 확인한다. (iv)서버 응용부는 값($g^x+(g^y)^v(\mathrm{mod}p)$)와 값($(g^x)^y(\mathrm{mod}p)$)의 해쉬값(hash2)을 구해서 클라이언트 응용부에 전송한다. (iv) 클라이언트 응용부는 해쉬값(hash2)을 구해서 수신된 해쉬값과 비교한다. (v) 클라이언트 응용부는 값이 일치할 경우 사용자 인증 사실을 확인하고 서버를 인증하는 한편, 키($g^{(xy)}(\mathrm{mod}p)$) 일치 사실을 확인한다.

발명의 효과

구현상의 경제성과 용이성을 갖는 패스워드인증방법은 상업적인 정보의 전송이 크게 증가하고 있는 인터넷과 같은 환경에서 계속 요구되고 또한 사용될 전망이다. 본 발명으로 인하여 안전하고 효과적인 사용자 인증 및 키 일치 기능을 다양한 서비스 환경에서 제공할 수 있다.

(57) 청구의 범위

청구항 1.

발명의 구성 3항의 [도해 3]의 사용자 인증 방법 ①②③④⑤.

① 사용자가 클라이언트 응용부에 아이디(id)와 패스워드(s)를 입력한다.

② 클라이언트 응용부가 서버 응용부에 아이디(id)와 난수(a)를 전달한다.

③ 서버 응용부가 클라이언트 응용부에 값 (s XOR t, $g^y+a*g^v(\mathrm{mod}p)$)를 전달한다.

④ 클라이언트 응용부가 서버 응용부에 값 ($g^x+(g^y)^v(\mathrm{mod}p)$, h($g^y+a*g^v(\mathrm{mod}p)$, $(g^y)^x(\mathrm{mod}p)$))를 전달한다.

⑤ 서버 응용부가 클라이언트 응용부에 값(h($g^x+(g^y)^v(\mathrm{mod}p)$, $(g^x)^y(\mathrm{mod}p)$))를 전달한다.

청구항 2.

발명의 구성 2항의 [도해 2]의 온라인 등록 방법 ①②③④⑤⑥.

① 사용자가 클라이언트 응용부에 아이디(id)와 패스워드(s)를 입력한다.

② 클라이언트 응용부가 서버 응용부에 값(id, $g^r(\mathrm{mod}p)$, {s XOR k1($(g^z)^r(\mathrm{mod}p)$)} _k2($(g^z)^r(\mathrm{mod}p)$))을 전달한다.

③ 서버 응용부가 클라이언트 응용부에 값(s XOR t, $g^y+a*g^v(\mathrm{mod}p)$)를 전달한다.

④ 클라이언트 응용부가 서버 응용부에 값($g^x+(g^y)^v(\mathrm{mod}p)$, h($g^y+a*g^v(\mathrm{mod}p)$, $(g^y)^x(\mathrm{mod}p)$))를 전달한다.

⑤ 서버 응용부가 클라이언트 응용부에 값(h($g^x+(g^y)^v(\mathrm{mod}p)$, $(g^x)^y(\mathrm{mod}p)$))를 전달한다.

⑥ 서버 응용부는 패스워드자료저장공간에 값(id, s XOR t, $g^v(\mathrm{mod}p)$)를 저장한다.

청구항 3.

청구항 제1항의 ③의 메시지 구성 방법.

③ s XOR t, $g^y+a*g^v(\mathrm{mod}p)$

청구항 4.

청구항 제1항의 ④의 메시지 구성 방법.

④ $g^x+(g^y)^v(\mathrm{mod}p)$

청구항 5.

청구항 제2항의 ②의 메시지 구성 방법.

② {s XOR k1($(g^z)^r(\mathrm{mod}p)$)}_k2($(g^z)^r(\mathrm{mod}p)$)

청구항 6.

청구항 제1항의 ②③과 청구항 제3항의 난수(a)를 삭제할 수 있는 방법.

② id

③ s XOR t, $g^y+g^v(\mathrm{mod}p)$

청구항 7.
청구항 제1항의 ③④⑤와 청구항 제2항의 ③④⑤⑥과 청구항 제3항과 청구항 제4항의 함수f(s,t)의 구성 방법.

f(s,t)= h(t,h(s,t)) . h(s,t)

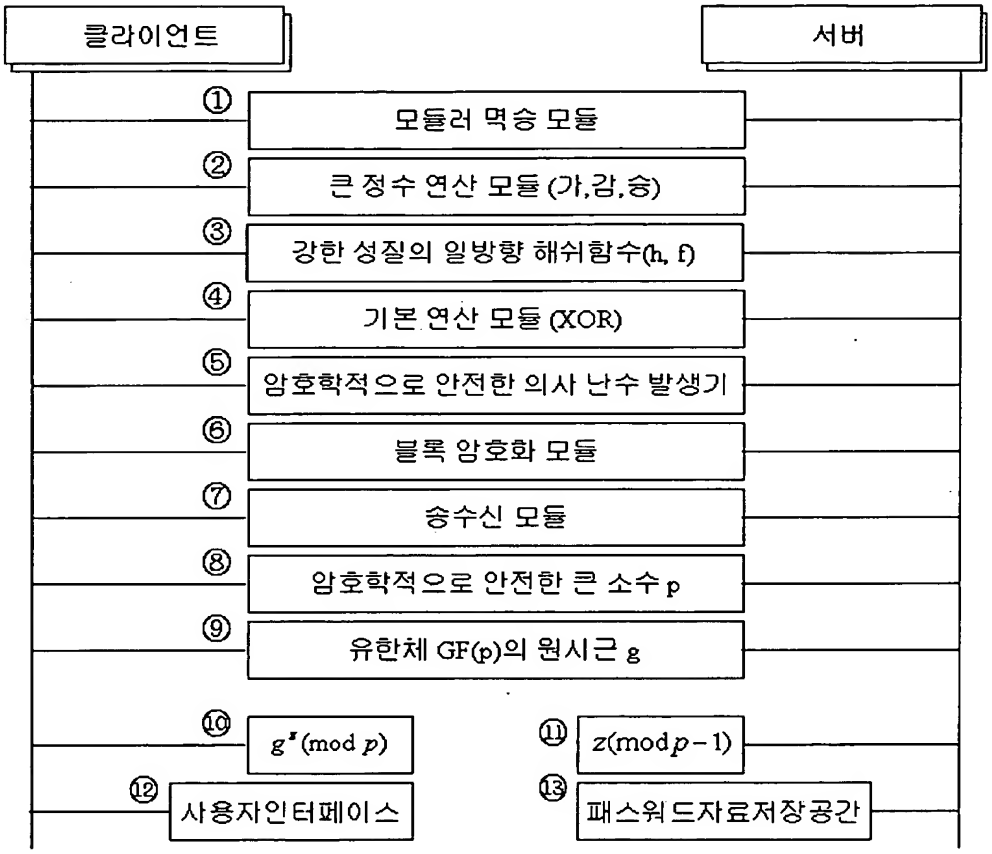
청구항 8.
청구항 제2항의 ②의 함수 k1(x)과 k2(x)의 구성 방법.

k1(x)는 x의 msb(most significant bit)부터 패스워드(s) 크기 만큼의 비트열을 선택한다.

K2(x)는 x의 lsb(list significant bit)부터 블록암호화알고리즘의 키 크기 만큼의 비트열을 선택한다.

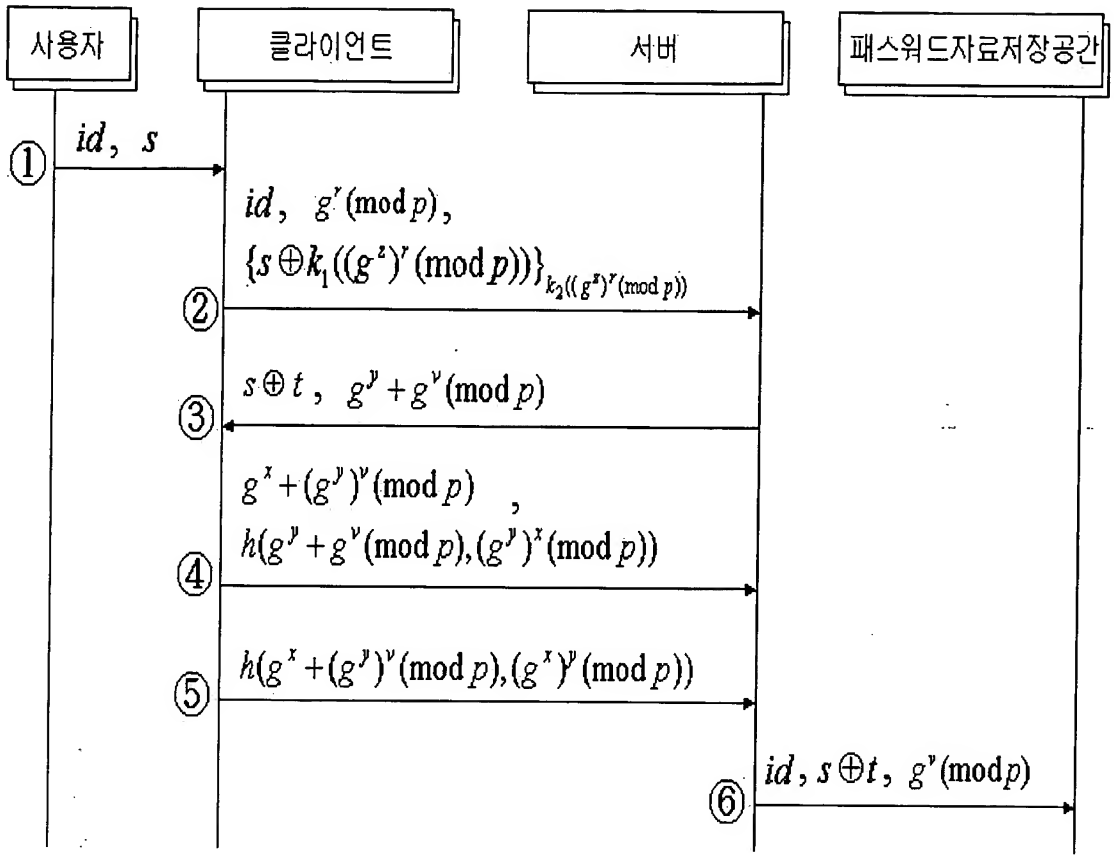
도면

도면 1



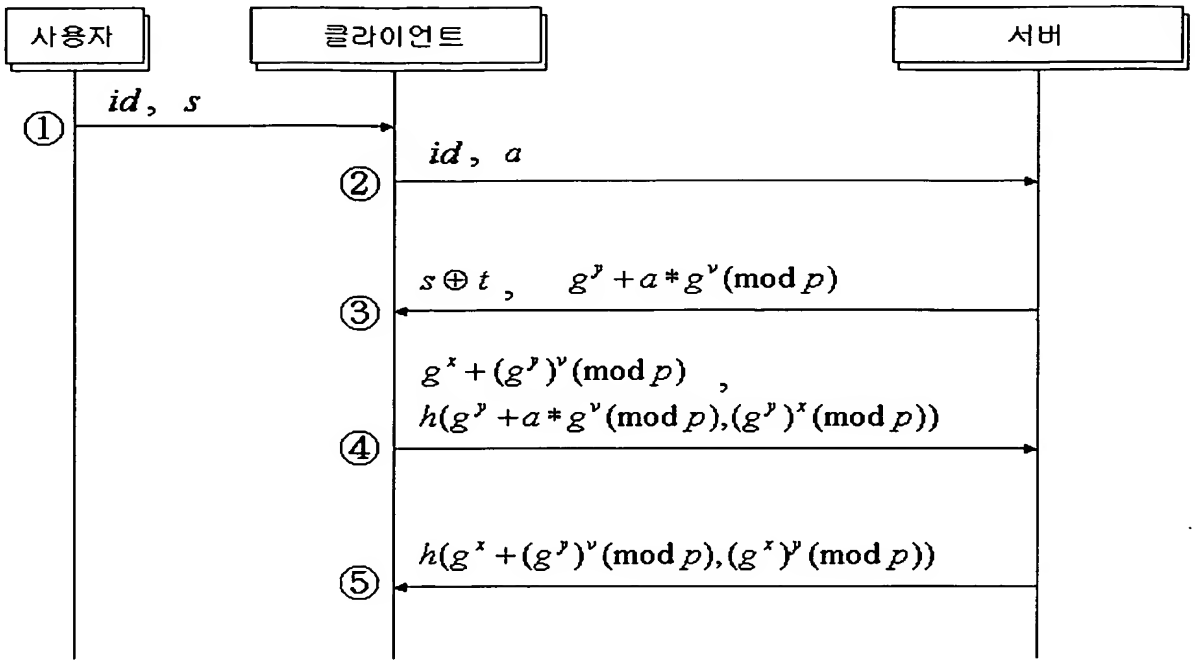
[도해 1] 인증시스템 구조

도면 2



[도해 2] 온라인 등록 절차

도면 3



[도해 3] 인증 프로토콜